

IN THE CLAIMS

1(currently amended). A promotion issuing system having fraud preventative measures,
comprising:

a first computer connected to a network, the first computer having a memory;

at least one additional computer connected to the network, the at least one additional
5 computer having a memory; and

a first process that resides in the first memory of the first computer with instructions
to:

(a) distribute a promotion on the network;

(b) identify the downloading of the promotion by the at least one
10 additional computer and associate a first fraud preventative data
structure with the promotion;

(c) allow the at least one additional computer to download the
promotion, if security software residing on the at least one additional
computer has not detected the first data structure more than once;

(d) terminate any further attempts by the at least one additional computer
15 to download the promotion any additional times;

(e) associate a fraud preventative second data structure with the promotion and display a symbol of the data structure on the promotion if the promotion is printed; and

20

(f) communicate a copy of the second data structure to a clearinghouse that can compare the copy to the symbol on the promotion.

2(canceled).

3(previously presented). The system of claim 1 wherein the security software has instructions to record first data structure associated with the promotion about the promotion, and communicate with the first process in the determination to allow the download if the first data structure has been recorded and to terminate the download if the first data structure has
5 been recorded any additional times.

4(previously presented). The system of claim 1, wherein the security software has instructions to:

identify the at least one additional computer each time the at least one additional computer attempts to download the promotion,

5

allow the at least one additional computer to download the promotion if it has been identified once, and

terminate any additional downloads if the at least one additional computer has been identified more than once.

5(Previously presented). The system of claim 1 wherein the first data structure is stored in the memory of the first computer, and a copy of the first data structure is stored in the at least one additional computer.

6(Previously presented). The system of claim 5 wherein the first computer is adapted to allow the at least one additional computer to download the promotion and record the copy of the first data structure, and terminate any further download attempts made by the at least one additional computer if the first data structure is recorded in the memory of the first computer any additional times.

7(Previously presented). The system of claim 1 further comprising a device coupled to the first computer and the at least one additional computer, the device being adapted to disallow more than one download of the promotion by the at least one additional computer.

8(Currently amended). A method of managing on-line promotions and preventing fraudulent use of the promotions, comprising:

using a first computer to distribute a plurality of promotions on a network, wherein the promotions are adapted to be downloaded by a plurality of computers,

5 tracking each of the plurality of promotions that are downloaded on one or more of the plurality of computers, by providing a front end security measure using a first fraud preventative data structure and providing a back end security measure using a second fraud preventative data structure associated with each the promotions,

10 identifying and terminating attempts to download any one of the plurality of promotions more than once on any one of the plurality of computers, by tracking the fraud preventative first data structure, and

identifying and terminating attempts at redeeming fraudulently copy of any of the promotions by tracking the second fraud preventative data structure.

9(original). The method of claim 8, wherein the plurality of promotions are available to one or more of a plurality of network locations.

10(original). The method of claim 9 wherein the network locations are web sites.

11(previously presented). The method of claim 9 wherein the first data structure of each of the plurality of promotions is tracked by security software that resides on each of the one or more of the plurality of computers.

12(previously presented). The method of claim 11 further comprising storing the first data structure associated with each of the plurality of promotions on the first computer, and additionally storing the first data structure in the security software.

5 13(previously presented). The method of claim 12 wherein identifying and terminating attempts to download the promotion more than once, further comprises allowing any one of the plurality of computers to download any one of the plurality of promotions if the security software matches its stored first data structure with the stored first data structure in the first computer, and disallowing any one of the computers to download any one of the promotions if the security software matches its first data structure with the first data structure in the first computer any additional times.

14(previously presented). The method of claim 11 further comprising using the security software to identify components of each of the plurality of computers, and storing data corresponding to the components in the security software and on the first computer.

15(original). The method of claim 14 wherein identifying and terminating attempts to download the promotion more than once, further comprises allowing any one of the plurality of computers to download any one of the plurality of promotions if the data corresponding to the components matches with the data corresponding to the components on the first

5 computer, and disallowing any one of the computers to download any one of the promotions if the data corresponding to the components matches with the data corresponding to the components on the first computer any additional times.

16(previously presented). The method of claim 9 wherein each of the plurality of promotions is tracked by a cookie that resides on one or more of the plurality of computers.

17(original). The methods of claim 9 wherein each of the plurality of promotions is tracked by a device coupled to the first computer and to each of the plurality of computers.

18(original). The method of claim 9 further comprising limiting the duration that the promotion can be validly downloaded by one of more of the plurality of computers.

19(previously presented). The method of claim 9 wherein associating the second data structure with each of the plurality of promotions, helps to determine if there exists a copy of any one of the plurality of promotions and to disallow the copy to be redeemed.

20(currently amended). A method of preventing abusive use of an on-line promotion, comprising:

providing the promotion with a unique identifier in the form of a fraud
preventative data structure stored on a computer of a user attempting to
download the promotion,

distributing security software to a computer that is attempting to download the
promotion,

using the security software to record the identifier,

denying a download if the security software has recorded the identifier more than
once,

optionally printing the promotion if the download has not been denied,

providing the printed promotion with a second unique identifier that is printed on the
promotion,

providing a promotion clearing house with a copy of the second unique identifier in
the form of a second fraud preventative data structure,

checking the printed promotion for copying, by comparing the unique printed
identifier on the promotion with the copy of the unique printed identifier, and

denying redemption of the promotion if the copy of the second unique identifier has
already been successfully compared with the second unique identifier from
a different promotion.